12-6-04

IFW 3713

Express Mail Label No. Dated: _____

Docket No.: 03795/000J514-US0
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Harold Cote et al.

Application No.: 09/891,875 Confirmation No.: 9036

Filed: June 25, 2001 Art Unit: 3713

For: COMPUTER GAMBLING GAME Examiner: K. T. Nguyen

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Canada	2,258,809	December 23, 1998

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: December 3, 2004

Respectfully submitted,

By Laura C. Brutman

Laura C. Brutman
Registration No.: 38,395
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 753-6237 (Fax)
Attorneys/Agents For Applicant

Application No. (if known): 09/891,875 Attorney Docket No.: 03795/000J514-US0

Certificate of Express Mailing Under 37 CFR 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. EV382051438-US in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on December 3, 2004
Date

Signature

D Beck
Typed or printed name of person signing Certificate

Registration Number, if applicable

Telephone Number

Note: Each paper must have its own certificate of mailing, or this certificate must identify each submitted paper.

Claim for Priority and Submission of Documents (1 page)
Certified Copy of Priority Document (Canadian Patent No. 2,258,809) (38 pages)
Return Receipt Postcard

Office de la propriété intellectuelle du Canada

Un organisme d'Industrie Canada

Canadian Intellectual Property Office

An Agency of Industry Canada

Bureau canadien des brevets

Certification

Canadian Patent Office

Certification

La présente atteste que les documents ci-joints, dont la liste figure ci-dessous, sont des copies authentiques des documents déposés au Bureau des brevets.

This is to certify that the documents attached hereto and identified below are true copies of the documents on file in the Patent Office.

Mémoire descriptif et dessins, de la demande de brevet no: **2,258,809**, tels que déposés, le 23 décembre 1998, par **LOTO-QUÉBEC**, cessionnaire de Harold Côté et Stephan Giard, ayant pour titre "Jeu de Hasard et D'Argent sur Ordinateur".

CERTIFIED COPY OF PRIORITY DOCUMENT

L. Gregoire

Agent certificateur/Certifying Officer

29 juin 2001

Date

Canada

(CIPO 68)
01-12-00

OPIC CIPO

PRÉCIS DE LA DIVULGATION

Un jeu de hasard et d'argent pour ordinateur utilisant un billet de loterie de type instantanée est décrit dans la présente demande. Le billet de loterie comprend une amorce, un code à barres et, optionellement, des codes secondaires. Un cédérom comprenant un programme d'ordinateur fait également partie de la présente invention. Le programme d'ordinateur reçoit l'amorce et la décode pour obtenir un germe. Un algorithme du programme d'ordinateur permet de déterminer le déroulement et l'issue d'un jeu à partir dudit germe. La portion jeu du programme d'ordinateur est alors activée en ayant le germe comme entrée et le jeu se poursuit jusqu'à l'issue finale. Si le billet est gagnant, l'issue du jeu sera un gain et le joueur sera invité à retourner le billet gagnant à l'opérateur pour réclamer son lot. La nature du lot est inscrite dans le code à barres du billet de loterie.

TITRE DE L'INVENTION

JEU DE HASARD ET D'ARGENT SUR ORDINATEUR

DOMAINE DE L'INVENTION

La présente invention a trait aux jeux de hasard et d'argent. Plus spécifiquement, la présente invention a trait aux jeux de hasard et d'argent pouvant être joués par ordinateur.

DESCRIPTION DE L'ART ANTÉRIEUR

Le monde traditionnel des Jeux de hasard et d'argent (ci-après «JHA») est basé sur un contrôle complet du jeu par l'opérateur (le plus souvent une Société de Loterie Nationale ou un de ses mandataires). Que ce soit des jeux de type «loterie», par tirage ou en mode instantanée («scratch & win»), des jeux de tables de type casino, ou encore des jeux sur machines, de type machine à sous ou «vidéo», l'opérateur exerce un contrôle direct sur tous les aspects du jeu : prises des mises ou paris, émissions des billets ou reçus de participation, tirages et choix des gagnants, interface visuelle et déroulement du jeu, paiement des lots, etc. Ce contrôle est nécessaire pour assurer l'intégrité du jeu et éliminer les risques de fraudes.

La disponibilité récente d'ordinateurs sophistiqués au domicile ouvre de nouvelles opportunités pour le marché du JHA.

Cependant, un ordinateur personnel, sur lequel un utilisateur a plein contrôle, peut difficilement être considéré suffisamment sécuritaire pour permettre le JHA.

Des inventions déjà protégées par brevet, par exemple les brevets américains portant les numéros 5,569,082 et 5,709,603, émis à M. Kaye, utilisent le concept d'un code qui détermine les résultats d'un jeu, mais les concepts développés par M. Kaye impliquent un médium «sécuritaire» de support, ce médium n'étant pas précisé ou son utilisation pas assez détaillée pour permettre de résoudre tous les problèmes opérationnels sous-jacents.

OBJETS DE L'INVENTION

Un objet de la présente invention est donc de présenter un jeu de hasard et d'argent sur ordinateur amélioré.

BRÈVE DESCRIPTION DES FIGURES

La Figure 1 est un bloc diagramme représentant le processus général d'opération de l'invention;

La Figure 2 est un bloc diagramme représentant le processus du point de vue du joueur;

Les Figures 3, 3A et 3B constituent un bloc diagramme illustrant l'opération détaillée du jeu;

Les Figures 4 et 4A constituent un bloc diagramme illustrant l'opération de publication d'un nouveau jeu; et

Les Figures 5 et 5A sont des vues schématiques illustrant un billet de loterie.

DESCRIPTION DÉTAILLÉE DE L'INVENTION

Afin de bénéficier de l'interface sophistiqué que représente l'ordinateur (présentation multimédia, interaction avec le joueur), la présente invention permet la vente de JHA sur ordinateur personnel tout en garantissant un plein «contrôle» à l'opérateur, i.e. la Société de Loterie Nationale.

Le contrôle du JHA est garanti par l'usage de billets de loterie traditionnelle de type instantanée («scratch & win»). Ces billets contiennent, sous la partie protégée par une couche de latex, un code, ci-après appelé «Amorce», qui permet le contrôle d'un jeu opéré sur l'ordinateur personnel du joueur. Cette Amorce est entrée dans l'ordinateur par le joueur dès le démarrage du jeu et indique au jeu comment doit se dérouler la partie jusqu'à son issue finale. L'Amorce détermine l'issue du jeu peu importe l'interaction avec le joueur. De cette manière, le billet contenant l'Amorce peut être associé à un lot à l'avance,

ce lot correspondant exactement à l'issue donnée lorsque l'Amorce est jouée.

La validation du billet permet au joueur d'obtenir son lot s'il a gagné, comme dans le cas des billets traditionnels de loterie. Tous les risques associés aux fraudes impliquées par la manipulation du jeu sur ordinateur sont éliminés par l'invention, puisque c'est le billet de loterie qui est payable au porteur.

L'invention prend un soin particulier à résoudre plusieurs problèmes soulevés par une analyse détaillée du concept, à savoir:

- les risques d'erreur du joueur : mauvais jeu utilisé avec un billet (ou vice versa), erreur de saisie de l'Amorce, etc.;
- les risques de différences entre l'issue annoncée par le jeu sur ordinateur et le lot associé au billet de loterie correspondant;
- les risques associés aux manipulation du jeu : paiement des lots, fausses réclamations, fausses prétentions du joueur face à l'issue, etc.;
- l'attaque de la programmation informatique du jeu pour découvrir des Amorces valides qui permettraient de jouer pour le divertissement (ce qui au niveau commercial peut être jugé problématique);
- les risques de transcriptions et diffusions d'Amorces valides (pour permettre le jeu pour divertissement);

- les risques de trouver des Amorces valides par essais et erreurs (pour permettre le jeu pour divertissement); et
- la gestion de l'achat des participations et de la réclamation des lots.

De plus, l'invention permet d'optimiser la flexibilité de l'ordinateur en n'établissant aucune contrainte entre l'Amorce et les scénarios de jeu possible sur l'ordinateur. En effet, l'Amorce ne contient aucune information qui permet de décoder ce que sera le déroulement d'une partie et son issue finale. Elle identifie plutôt une valeur «initiale» de partie, ci-après appelée le «Germe», qui elle, permet de contrôler le déroulement de la partie. De plus, ce Germe ne contient pas lui-même, encodé dans sa valeur, la description explicite du déroulement de la partie et de l'issue. Le déroulement complet d'une partie dépend donc du Germe initial mais ce déroulement ne peut être interprété du Germe lui-même par analyse. Il faut «jouer» le Germe pour connaître le déroulement qu'il implique.

Cette approche très ouverte, i.e. aucune contrainte n'est imposée sur le contenu de l'Amorce et du Germe, permet d'obtenir les avantages suivants:

- les Amorces peuvent être déterminées sans tenir compte du nombre de jeux en circulation, du nombre de lots possibles ou tous autres paramètres de jeu, ce qui peut être rapidement très contraignant;

- l'analyse des Amorces ne donne aucune information sur la manière de générer des Amorces valides;
- le lien qui unit l'Amorce à un Germe, et donc à l'issue de la partie, est aléatoire et non analysable;
- les Germes n'ont pas un format lié aux jeux et aux paramètres qui gouvernent son déroulement, ce qui implique que l'invention peut donc être appliquée à n'importe quel modèle de jeu;
- le lien entre le Germe et l'issue de la partie, donc le «lot gagné» si la partie est gagnante, est unidirectionnel, i.e. qu'on ne peut remonter au Germe à partir d'une issue spécifique de partie; cet attribut conserve un aspect aléatoire aux Germes utilisés: on ne peut donc reconstruire les Germes en usage pour un jeu à partir de la structure de lots annoncée.

Un mode préféré de réalisation de la présente invention sera maintenant décrit à titre purement indicatif.

Se référant au bloc diagramme de la Figure 1, le processus général selon un mode préféré de la présente invention sera maintenant décrit.

Dans le bloc 101, un processus informatisé, contenu dans un serveur sécurisé, génère les informations nécessaires à la publication d'un nouveau jeu selon des paramètres spécifiques (nombre de parties, structure de lots, etc). Ce processus génère d'une part un

ensemble d'Amorces et d'autre part, des Germes de partie. Les Amorces sont liées de manière unique à chaque Germe.

Dans le bloc 102, les Amorces générées dans le bloc 101 sont imprimées sur des billets de loteries traditionnels de type instantanée. L'Amorce remplace la surface de jeu sous le latex où l'on retrouve normalement des symboles à assortir.

Dans le bloc 103 les Germes générés dans le bloc 101 sont brouillés et stockés dans un fichier informatique. Ce fichier est écrit sous forme de table sur les cédéroms, ci-après «CD», contenant les programmes de jeu eux-mêmes.

Il est à noter que les étapes décrites dans les blocs 101, 102 et 103 seront décrites de façon plus spécifiques aux Figures 4 et 4A.

On distribue ensuite les billets et les CD dans le réseau de vente traditionnel de la Loterie (bloc 104). On pourra vendre des paquets CD-Billets et des billets seuls pour les joueurs qui auront déjà le CD.

Une fois qu'il s'est procuré le CD et au moins un billet, le joueur installe le programme contenu sur le CD dans son ordinateur et le démarre (bloc 105). Il suit les instructions du jeu pour saisir les Amorces se trouvant sur les billets de loterie qu'il a achetés avec le CD. Le jeu lui permettra une partie pour chaque Amorce achetée. À la fin de chaque partie, le jeu indiquera au joueur s'il gagne un lot quelconque et

l'invitera, le cas échéant, à aller faire valider le billet de loterie correspondant.

Le joueur ramène les billets de loterie qui ont été déclarés gagnants par le jeu au point de vente. Le vendeur validera les billets et paiera le gagnant (bloc 106).

Se référant maintenant à la Figure 2 qui précise les blocs 104, 105 et 106, le processus du point de vue du joueur sera maintenant décrit.

Au bloc 201, le joueur se rend au point de vente traditionnel de billets de loterie et achète un ou plusieurs billets de loterie identifiés. S'il n'a jamais joué au jeu, il achètera un paquet de démarrage qui contient le CD du jeu et un ou plusieurs billets. S'il possède déjà le CD du jeu, il n'achètera que de nouveaux billets. Plusieurs jeux pouvant être disponibles, les CD et billets seront facilement identifiés pour chaque jeu avec des «noms» et des «images» appropriés.

Le joueur installe ensuite, au bloc 202, le jeu contenu sur le CD sur son ordinateur personnel selon la procédure conventionnelle pour ce genre d'opération. Parmi les paramètres d'installation, le joueur pourra choisir de mettre en place un contrôle d'accès au jeu pour en limiter l'utilisation (par le reste de sa famille, les enfants, ou d'autres personnes utilisant le même ordinateur). Lorsqu'il est prêt à jouer, le joueur démarre le jeu installé ; le CD doit alors être dans le lecteur de son ordinateur. Le jeu procède à certaines vérifications, comme l'intégrité du CD ou de certains paramètres qui s'y

trouvent (comme, par exemple, la table des Germes qui sera décrite ci-dessous au bloc 415).

Le jeu s'authentifie avec le «nom» du jeu et des «images» appropriées. Le joueur pourra ainsi reconnaître que le jeu démarré est celui qui correspond aux billets de loterie qu'il s'apprête à jouer (voir Figures 5 et 5A). Au bloc 203, le jeu demande au joueur de gratter le latex (voir 501, Figure 5) d'un billet de loterie qu'il s'est procuré et de saisir l'Amorce qui se trouve dessous (voir 506, Figure 5A) dans les cases affichées à l'écran de l'ordinateur. Afin de réduire les risques de mauvaises saisies, le jeu fournit un clavier à cliquer avec la souris à l'écran. De plus l'Amorce peut contenir des symboles qui n'apparaissent pas sur un clavier d'ordinateur standard. Ces symboles, s'ils changent pour chaque jeu, permettent d'assurer que le joueur n'essaie pas de saisir une Amorce pour le mauvais jeu, puisqu'alors il ne pourra saisir les symboles qui sont sur son billet. L'utilisation de symboles et de lettres en alternance permet aussi de limiter les erreurs de saisie simple (e.g.: la position «deux» de l'Amorce saisie pour la «trois»). Dans certaines variantes, une deuxième surface de symboles sous latex (voir 503, Figure 5) sera disponible sur le billet (code secondaire). À l'invitation du jeu, le joueur devra gratter l'un des cases de cette deuxième surface contenant les codes secondaires et saisir les symboles qui s'y trouvent (voir 507, Figure 5A). Ces symboles compléteront la valeur totale de l'Amorce.

Après confirmation de la fin de saisie de l'Amorce par le joueur, le jeu l'analyse et la valide (bloc 204). L'Amorce saisie en symboles est, bien entendu, convertie en format binaire pour fins d'analyse. Certains des bits de l'Amorce peuvent être des informations

qui permettent de vérifier qu'il n'y a pas eu d'erreur de saisie («check digit»). L'Amorce est ensuite manipulée pour obtenir un index dans la table des Germes de partie qui se trouvent sur le CD du jeu. L'index permet d'identifier lequel des Germes de la table le jeu utilisera pour contrôler le déroulement de la partie et l'issue finale. L'entrée dans la table contient des informations de validation supplémentaires en plus du Germe lui-même. Ces informations permettent d'assurer que l'Amorce saisie est la bonne et limite les chances de tomber par essais et erreurs sur une Amorce valide.

Ces validations effectuées, le jeu initie la partie en prenant le Germe pointé par l'Amorce saisie comme paramètre de départ (bloc 205). Ce paramètre de départ déterminera le déroulement de toute la partie et l'issue finale. Selon le type de jeu, le joueur pourra être appelé à participer ou non. Peu importe la participation du joueur, le jeu se terminera toujours par l'issue finale déterminée dans le Germe de départ.

À la fin de la partie, le jeu annonce au joueur, au bloc 206, le résultat final, i.e. l'issue de la partie. Le joueur peut être gagnant ou non. Les lots peuvent être de différentes natures : prolongation de partie, parties gratuites, biens, montants en argent, etc.

Au bloc 207, si le joueur est déclaré gagnant, il conserve le billet de loterie qui contenait l'Amorce de cette partie et le présente au point de vente de la Loterie.

Le vendeur de loterie validera le billet grâce au système de validation traditionnel de la Loterie et paiera le lot gagné par le joueur selon les messages reçus du système (bloc 208).

Il est à noter que les étapes des blocs 203 à 208 seront décrites ci-dessous de façon plus détaillée aux Figures 3, 3A et 3B.

Se référant maintenant aux Figures 3, 3A et 3B, l'opération détaillée du jeu sera maintenant décrite.

Le bloc 301 est similaire au bloc 203 décrit ci-dessus et concerne le grattage du latex et l'entrée de l'amorce.

Au bloc 302, la conversion d'une Amorce, indiquées en symboles sur le billet, en valeur binaire permet une meilleure flexibilité au niveau programmation dans le jeu. Les symboles utilisés peuvent être des lettres, des chiffres ou tous autres symboles facilement identifiables, comme les symboles de cartes à jouer, des symboles géométriques, des objets simples ou stylisés. Selon le nombre de parties possibles pour un jeu et donc le nombre de billets de loterie imprimés, l'Amorce devra être plus ou moins longue afin de couvrir l'ensemble de toutes les valeurs possibles. Par exemple, une Amorce composée de 3 lettres de l'alphabet romain (A-Z), ne permet que 26*26*26 Amorces différentes, soit 17576. Si on veut vendre plusieurs centaines de milliers de billets pour un jeu, l'Amorce devra être suffisamment longue pour le permettre. Une variante de cette approche est de réutiliser les mêmes valeurs d'Amorces sur plusieurs billets. Tous ces billets ayant la même Amorce fourniront toutefois le même déroulement de partie et la même issue.

Afin de réduire les risques que quelqu'un joue pour le divertissement, il doit être difficile de calculer ou déduire toute Amorce correspondant à un Germe dans la table des Germes contenue sur le CD. Comme l'Amorce sert à retrouver le Germe de la partie, il faut utiliser un algorithme non réversible (bloc 303), i.e. un algorithme qui se calcule aisément dans une direction (de l'Amorce vers le Germe), mais pas dans l'autre direction (du Germe vers l'Amorce). On obtiendra donc l'index de la table des Germes en appliquant un algorithme non réversible à l'Amorce (ou à une partie de celle-ci). Parmi les techniques que l'on peut utiliser, il y a des «ou exclusifs» avec des séries de bits aléatoires, des algorithmes standards de chiffrage à clé publique, comme RSA ou DSA, ou encore des algorithmes de génération d'empreintes de messages (Message Digest), comme MD5 ou SHA. Peu importe la technique utilisée, il faut s'assurer que l'algorithme appliqué à une Amorce donnera toujours un résultat unique pour l'ensemble des Amorces possibles dans le jeu. Il doit y avoir une relation biunivoque (un à un) entre chaque Amorce et chaque Germe de la table du CD. Le choix de l'algorithme aura aussi des conséquences sur le processus de génération des Amorces (voir description détaillée de la figure 4). Dans certains cas, selon les algorithmes choisis, la longueur de l'Amorce devra être augmentée pour permettre l'unicité des résultats (on ne retiendra alors que les Amorces qui donnent des résultats différents).

L'index obtenu à partir de l'Amorce au bloc 303, sert à identifier une entrée dans la table des Germes du CD au bloc 304. Afin de réduire les chances de décodage de cette entrée, elle est brouillée, i.e. manipulée au niveau binaire, par un algorithme qui utilise l'Amorce correspondante en entrée. Encore une fois, on pourra utiliser, au choix,

des algorithmes standards, comme le DES ou RC4, pour brouiller l'entrée de la table, l'Amorce, ou une partie de celle-ci, étant utilisée comme clé de chiffrage. On pourra aussi générer une empreinte de message (message digest) à partir de l'Amorce, et faire un «OU EXCLUSIF» du résultat avec l'entrée de la table des Germes pour la débrouiller. L'important est d'utiliser l'Amorce dans ce brouillage afin qu'il ne soit pas possible de débrouiller l'entrée sans connaître l'Amorce originale qui a été associée au Germe lors du processus de création du jeu (voir figure 4). La seule attaque possible demeure alors l'essai systématique de toutes les Amorces possibles.

L'entrée débrouillée de la table des Germes contient le Germe lui-même, un code de lot et des informations de validation de l'Amorce. Les informations de validation de l'Amorce pourront être des empreintes totales ou partielles de l'Amorce originale (MD5, SHA, etc.). Pour valider l'Amorce (bloc 305), il s'agit de rappliquer l'algorithme de validation à l'Amorce saisie par le joueur et de comparer le résultat avec les informations dans la table des Germes. L'Amorce elle-même pourra contenir des bits de vérification («check digits»).

Au bloc 306, le jeu valide donc l'Amorce saisie avec les informations de la table et si les résultats sont négatifs, il demande au joueur de saisir son Amorce de nouveau (bloc 307). Une Amorce mal saisie, ou entrée au hasard, produira nécessairement un index de table de Germes (303). Les probabilités que cet index contienne des informations de validation qui corroborent «par hasard» l'Amorce saisie dépendront des algorithmes utilisés au blocs 302, 303 et 304, et de la longueur des informations de validation au bloc 305.

Bien entendu, le message affiché en cas de mauvaise saisie (bloc 307) devrait ne pas indiquer précisément quel symbole de l'Amorce est en faute, ou toute autre raison de mauvaise validation, ceci afin de ne pas faciliter le travail de quelqu'un qui cherche à trouver des Amorces valides par essais et erreurs.

Après les validations du bloc 306, le jeu utilise le Germe de l'entrée pointée par l'Amorce saisie pour «jouer la partie» une première fois, à l'insu du joueur (bloc 308). Avec la puissance des ordinateurs d'aujourd'hui, et sans la nécessité d'afficher le déroulement de la partie au joueur, ce processus devrait être suffisamment rapide et pour ne pas être «perçu» par le joueur. Au bloc 309, l'issue de la partie ainsi obtenue est comparée au code de lot contenu dans l'entrée du Germe obtenu en 305. Le code de lot est un valeur binaire qui représente une issue possible du jeu. On choisira un code suffisamment long pour exprimer toutes les issues possibles. Ce code de lot étant brouillé dans la table des Germes, on ne peut identifier quelles entrées donneront des issues gagnantes ou pas.

Si l'issue de la partie jouée à l'insu du joueur ne correspond pas au code de lot, on demande au joueur de saisir son Amorce de nouveau (bloc 307). Cette vérification permet d'assurer l'intégrité du Germe de l'entrée (i.e. qu'il n'y a pas eu d'erreur de lecture ou manipulation), et diminue encore plus les probabilités de ne pas diagnostiquer une erreur de saisie d'Amorce. En effet, le Germe et le code de lot étant brouillés par l'Amorce, les chances de tomber sur une Amorce qui valide en 306 et sur le code de lot mais qui ne soit pas l'Amorce originale correspondante sont très réduites.

Toutes ces validations effectuées, le jeu initie une partie en utilisant le Germe identifié par l'Amorce (bloc 310). Le déroulement de la partie est constitué d'un état initial et de changements de statuts jusqu'à une étape finale où le jeu est complété ou ne peut plus progresser. Chaque changement de statut à partir de l'état initial est dicté par le Germe identifié par l'Amorce. Le moteur du jeu qui génère les changements de statut à partir du Germe initial est construit sur le modèle d'un algorithme de génération pseudo-aléatoire, i.e. que tout état dépend de manière non réversible à la séquence de tous les états précédents à partir d'un germe initial (seed). Le Germe ne peut donc être calculé à partir du déroulement de la partie ou de son issue. Cette technique implique un processus spécial pour la génération de toutes les parties (décrit à la Figure 4) mais réduit les probabilités de générer des Germes valides et/ou pour une issue donnée. Il permet aussi de dissocier le format du Germe des paramètres du jeu. Cette flexibilité permet d'appliquer le principe à tous les modèles de jeu.

Le positionnement du jeu à l'étape finale, et/ou l'accumulation des événements survenus lors du déroulement de la partie (ex : l'accumulation de symboles de jeu ou des points ou des crédits) sont utilisés pour confirmer l'issue de la partie au joueur, i.e. s'il gagne quelque chose ou pas (bloc 311).

Le jeu indiquera au joueur gagnant, au bloc 312, que son billet doit être retourné au point de vente pour le faire valider et obtenir le lot gagné. À ce titre, le billet demeure un billet de loterie traditionnelle, tel que vendu par toutes les Loteries du monde.

Au bloc 313, le vendeur de loterie (ci-après appelé «l'opérateur») validera le billet grâce au code à barres, ou tout autre code similaire ou équivalent, qu'il contient (voir 502, Figure 5) et au terminal qui relie l'opérateur au système de validation de la Loterie. Si l'opérateur n'est pas muni d'un terminal le reliant au système de la Loterie, il pourra utiliser des codes spéciaux sur une zone spéciale du billet (voir 504, Figure 5) pour déterminer si le billet est gagnant et si oui, la nature du lot. Dans ce dernier cas, le billet devrait ensuite être acheminé à un centre de validation de la Loterie.

Grâce aux liens entre l'Amorce du billet, le Germe de la partie qui en détermine l'issue, et le code à barre qui identifie uniquement le billet, le système de validation de la Loterie sait quelle est l'issue de chaque partie jouée. La base de données centralisée de la Loterie (générée dans le processus décrit à la Figure 4) établit un lien entre les codes à barres des billets et les lots qui correspondent à leur Amorce. L'Amorce comme telle n'est pas maintenue dans cette base de données, ni le Germe du jeu correspondant, pour des raisons de sécurité (le personnel de la Loterie ne pourra publier des Amorces ou Germes valides). Seuls les billets gagnants d'un lot sont maintenus dans cette base de données. Donc, au bloc 314, le système de loterie utilise la base de données pour vérifier si le billet est gagnant.

Au bloc 315, le système de loterie détermine si le code à barres du billet correspond à une entrée dans la base de données de la loterie. Si tel est le cas, c'est que le billet correspond à une Amorce (et donc à un Germe) gagnant, un sémaphore indiquera si le billet a déjà été réclamé, i.e. s'il est déjà payé. S'il ne s'y trouve pas, c'est que le billet est

non gagnant. Ces vérifications sont standard pour les billets de loterie traditionnels.

Si le billet est non gagnant (bloc 316), s'il est déjà payé, ou encore si le code à barres est invalide (ces codes à barres contiennent des informations de validation pour en vérifier l'intégrité), alors le terminal de l'opérateur affiche et imprime un message à cet effet.

Si le billet est gagnant et non «déjà payé» (bloc 317), il est marqué «payé» dans la base de donnée. Cette sécurité standard avec les billets de loterie traditionnels permet d'assurer qu'on ne paie un billet gagnant qu'une seule fois. Ensuite, au bloc 318, un message du montant gagné par le billet est transmis au terminal de l'opérateur où il s'affiche et est imprimé sur un reçu. L'opérateur, au bloc 319, paie alors le montant indiqué au joueur et détruit le billet («cash&trash»).

Finalement, le système de gestion de la loterie sait que l'opérateur a payé le joueur et créditera le compte de l'opérateur du montant payé (bloc 320).

Se tournant maintenant vers les Figures 4 et 4A, l'opération de publication d'un nouveau jeu sera maintenant décrite.

Tout nouveau jeu doit faire l'objet d'une préparation avant d'être mis en marché. On doit décider combien de billets (et donc de parties) on mettra en vente et quelle sera la structure des lots, i.e. la répartition des revenus de la vente retournés aux joueurs sous forme de lots. Comme pour une loterie traditionnelle de type instantanée,

l'opérateur du jeu, i.e. une Société de Loterie Nationale, (ci-après la «Loterie») doit définir tous ces paramètres, en plus de décider d'autres considérations pouvant affecter le jeu ou son déroulement. Par exemple, on pourra décider que le déroulement de toute partie inclura l'apparente «forte probabilité» pour le joueur de gagner un gros lot («near miss»). Tous ces paramètres, ainsi que la structure de lots détaillée seront codés dans un fichier informatique au bloc 401.

Un programme informatique de la Loterie utilise le moteur du jeu (voir blocs 310 et 311) pour identifier des Germes qui donnent les résultats escomptés par le fichier des paramètres défini en 401. Aléatoirement, au bloc 402, le programme génère de Germes de partie et les joue. Il compare pour chaque partie ainsi jouée, les résultats obtenus, i.e. chaque étape du déroulement et l'issue finale, avec les résultats espérés et codés dans le fichier de paramètres au bloc 401. Ce processus peut démarrer avec un Germe initial et l'incrémenter à chaque essai ou procéder par sauts afin de générer un ensemble de Germes plus répartis.

Chaque fois que le programme obtient un Germe qui donne des résultats souhaités et non complètement satisfaits, il conserve ce Germe dans un fichier informatique avec l'issue de la partie qui lui correspond (bloc 403). Il marque le fichier des paramètres pour indiquer quels résultats ont été obtenus. Au choix, on pourrait conserver plus d'un Germe par résultat cherché afin d'obtenir un plus grand ensemble de Germes et Amorces à vendre.

Lorsque tous les paramètres sont satisfaits, le fichier des Germes et des issues est mélangé aléatoirement et disposé dans une table qui contient une entrée par Germe (bloc 404). Le mélange aléatoire permet de dissocier le processus de génération des Germes à leur séquence dans la table finale. Il sera impossible de retrouver un Germe dans la table par sa position même pour un programmeur qui connaîtrait le processus expliqué ci-dessus (bloc 402).

Afin de rendre la table des Germes plus robuste aux attaques de pirates informatique («hackers»), on ajoute, au bloc 405, des entrées invalides, i.e. qui ne correspondent à aucun Germe ou Amorce valide. Pour offrir une protection significative, le nombre d'entrées invalides devrait être au moins aussi élevé que celui des entrées valides. Les entrées invalides sont en fait une suite de bits générés aléatoirement. Ces entrées invalides sont distribuées aléatoirement parmi les entrées valides.

L'index d'une entrée est en fait sa position relative au début de la table. Par exemple, l'index d'un Germe valide placé en 3145^{e} position dans la table sera 3145. Les Germes valides étant mélangés avec les invalides, il y aura des sauts d'index. Un algorithme non réversible est ensuite utilisé, au bloc 406, pour trouver une valeur X qui donnera en sortie cet index (exprimé en valeur binaire). Par exemple, on pourra chercher quelle valeur binaire qui, chiffrée avec un algorithme comme DES, en utilisant cette même valeur comme clé de chiffrage, donnera la valeur de l'index (on pourra extraire la valeur de l'index du résultat si ce dernier est plus long que l'index). Ce processus étant basé sur essais et erreurs, il pourrait être très long. Aussi on peut considérer

travailler de manière globale en produisant en séquence des résultats pour différentes valeurs X, et ensuite retenir celles qui satisfont les index requis. Certains algorithmes tout aussi réversibles sont cependant plus faciles à utiliser. Par exemple, si l'index est exprimé comme une valeur binaire de 20 positions, on peut aisément générer une valeur X de 40 bits qui, lorsque ses deux moitiés sont additionnés par «OU EXCLUSIF», donnera l'index cherché. Cette valeur X ne pourra être calculée à partir de l'index si elle est générée comme suit : on génère les 20 premiers bits aléatoirement, on produit les 20 derniers bits en appliquant un «OU EXCLUSIF» entre cette première partie et la valeur de l'index elle-même. Une autre approche serait d'utiliser des algorithmes de chiffrage à clé publique, la valeur X serait alors produite en utilisant la clé privée sur l'index, et l'index pourrait être obtenu de la valeur X en utilisant la clé publique. L'usage d'algorithmes à clés publiques implique toutefois l'usage de série de bits relativement longue.

Au bloc 407, on insère dans l'entrée la valeur X obtenue en 406 pour chaque Germe valide de la table. Cette valeur servira à la validation de l'Amorce lors d'une vraie partie. Comme l'Amorce est en fait la valeur X formatée en symboles pour le billet, la retrouver dans l'entrée de la table des Germes permet de s'assurer que l'Amorce saisie est bel et bien celle générée par la Loterie et non un «alias» qui donnerait les mêmes résultats en appliquant les algorithmes non réversibles décrits au blocs 303, 304 et 305. L'usage d'algorithmes non réversibles rend en effet impossible l'assurance qu'une autre valeur en input (Amorce) ne donnera pas le même résultat en output (index). Le fait de pouvoir comparer la valeur originale de l'Amorce conservée dans la table des Germes élimine cette possibilité.

Pour chaque Germe valide, on exprime ensuite la valeur X en format d'Amorce, i.e. en suites de symboles qui seront éventuellement imprimés sur un billet de loterie (bloc 408). La correspondance des symboles aux valeurs binaires peut faire l'objet de variance d'un jeu à un autre, et même d'une position de l'Amorce à la suivante. Ces variances rendront la possibilité de trouver des Amorces valides plus difficiles. Dans certaines variantes, une partie de l'Amorce peut être exprimée dans un tableau de plusieurs symboles (voir 503 et 503, Figure 5). Le jeu ne demandera alors qu'un seul des caractères de ce tableau, mais aléatoirement (chaque symbole étant mathématiquement lié au numéro de la case pour correspondre toujours au même résultat en format binaire). Cette approche permet de réduire les chances que les Amorces soient transcrites et diffusées pour permettre à des joueurs de jouer pour le divertissement. En effet, un telle transcription serait plus longue, puisque le nombre de données à transcrire est supérieur, et rendrait le tout moins attrayant aux amateurs de divertissement.

Pour permettre la validation par le système de Loterie, chaque Amorce est ensuite associée à un numéro unique de billet au bloc 409. Ce numéro unique est indépendant de l'Amorce elle-même : il n'y a donc aucun moyen de calculer l'une des deux valeurs en ayant l'autre. Ce processus d'association est souvent effectué par l'imprimeur mandaté pour imprimer les billets de loterie. Le personnel de la Loterie n'a donc pas accès aux associations entre ces deux valeurs.

Ensuite l'impression traditionnelle de billets de type instantanée où on la surface de jeux sous le latex est remplacée par les

symboles de l'Amorce est effectuée au bloc 410. Les billets de loterie ainsi imprimés sont distribués selon les réseaux de ventes traditionnels de la Loterie (bloc 411). Une partie de ces billets sera emballée avec des CD de jeu. Les autres billets seront vendus individuellement.

Le numéro unique de chaque billet gagnant (inscrit dans le code à barres du billet, voir 502, Figure 5) est conservé avec le montant du lot dans la base de données du système centralisé de validation de la Loterie (bloc 412). Si c'est l'imprimeur qui associe le code à barres aux Amorces (et donc aux lots), ces informations sont transmises à la Loterie par l'imprimeur. Les Amorces ne se retrouvent pas dans cette base de données. Les billets qui contiennent des Amorces qui ne sont pas gagnantes ne sont pas inscrits dans cette base de données. Lors de la validation des billets, un code à barres non inscrit dans la base de données est automatiquement considéré non gagnant.

Tel que mentionné ci-dessus, la base de données des billets (voir bloc 413) est utilisée par le système de validation traditionnel de la Loterie. Le réseau de ventes de la Loterie permet à chaque détaillant opérateur d'utiliser un terminal de validation relié par un réseau à ce système central.

Puisque la table des Germes se retrouve sur le CD de jeu, il faut en protéger le contenu afin qu'un pirate informatique ("hacker") ne puisse calculer les Amorces ou Germes qui permettront de jouer des parties pour le divertissement. Au bloc 414, chaque entrée de la table des Germes est brouillée séparément à l'aide d'un algorithme réversible (pour permettre le débrouillage). Cet algorithme utilisera l'Amorce en

entrée pour faire varier le brouillage d'une entrée à l'autre et rendre difficile le débrouillage sans connaître l'Amorce originale correspondant à l'entrée. On pourra par exemple, générer une empreinte MD5 ou SHA sur l'Amorce (augmentée pour satisfaire la longueur minimale requise par l'algorithme) et appliquer le résultat en «OU EXCLUSIF» sur l'entrée contenant le Germe et les informations de validation (valeur X (bloc 407) et code de lot (bloc 404)). De cette manière, il faudra fournir l'Amorce originale pour débrouiller l'entrée.

La table des Germes brouillée est copiée sur chaque CD distribué avec les billets (bloc 415). Ce CD contient aussi le programme de jeu lui-même. Afin d'assurer l'intégrité du processus de production des CD, une empreinte globale de la table (MD5 ou SHA) pourra aussi y être ajoutée. Cette empreinte serait alors vérifiée lors du début du jeu (bloc 202).

Les CD (bloc 416) sont emballés avec des billets (bloc 411) pour la distribution, ou sont vendus séparément. Les CD n'ayant aucune valeur monnayable, on peut aussi les distribuer gratuitement pour stimuler la vente des billets qui permettent d'y jouer.

Les Figures 5 et 5A, décrites en détail ci-dessous, illustrent un billet de loterie selon un mode de réalisation de la présente invention.

Les billets de loterie sont des billets de type instantanée traditionnels («scratch & win»). La Figure 5 montre le billet 505 avant qu'il ne soit gratté, i.e. avec une couche de latex 501 recouvrant l'Amorce, et

la Figure 5A montre ce même billet après que la couche de latex 501 ait été grattée par le joueur.

La surface sur laquelle se trouve imprimée l'Amorce est protégée par une couche de latex 501 afin de ne pas pouvoir distinguer les billets qui seront gagnants avant l'achat. Un billet gratté ne peut être vendu. La surface en latex 501 est éprouvée dans le monde des loteries traditionnelles et permet la protection contre différentes techniques qui pourraient être utilisées pour lire sous la surface (éclairage, processus chimique, grattage et collage, etc). Un motif de couleur (non montré) est normalement imprimé sur la surface de latex 501 afin de rendre toute contrefaçon ou manipulation difficile.

Le code à barres 502 du billet contient un numéro qui identifie de manière unique chaque billet pour un jeu donné. Ce numéro peut être codé avec une hiérarchie d'informations : numéro de jeu, numéro de livrets, numéro d'émission, etc. Plusieurs formats standards de code à barres peuvent être utilisés selon la longueur du numéro encodé (128c, I2of5). Des formats plus denses, dits à deux dimensions, sont aussi disponibles. Les codes à barres contiennent normalement des valeurs de vérification qui permettent de diagnostiquer les erreurs de lectures. De plus le numéro lui-même peut contenir d'autres valeurs de vérification qui permettent la contrôler l'intégrité jusqu'à la réception par le système centralisé de validation de la Loterie.

La surface 507 du billet peut contenir des symboles de toute nature. Cette surface est optionnelle. Elle permet d'exprimer une partie de l'Amorce en un format qui est difficile à transcrire. Bien qu'une

seule case de cette surface sera saisie par le joueur, toute la table doit être disponible parce que le jeu choisit la case à entrer au hasard lors de la partie. Plus il y a de cases, plus il sera difficile de transcrire l'information du billet pour la diffuser et permettre le jeu pour le divertissement seulement. La surface 507 est recouverte d'une couche de latex 503.

La surface de latex 504 est courante dans les billets de loterie traditionnels. Sous le latex 504 se trouvent des codes qui permettent aux opérateurs de la Loterie d'identifier si un billet est gagnant et pour quel montant sans valider avec le système central de la Loterie. Cette information est utilisée si le système de validation est non disponible ou s'il y a un doute de contrefaçon. Cette surface ne doit jamais être découverte par le joueur.

Il est à noter que le reste du billet 505 est normalement imprimé en couleurs et motifs qui représentent le thème du jeu. En plus de réduire les possibilités de contrefaçon, cette impression permet d'associer les billets au jeu lui-même (et au CD).

Les symboles de l'Amorce 506 peuvent être disposés de plusieurs manières selon le nombre de symboles requis. Les symboles qui ne sont pas alphanumériques peuvent être accompagnés d'une courte description en petits caractères afin de rendre toute confusion impossible. Par exemple, on pourra écrire «ciseau» sous le symbole du ciseau.

Il va de soi que la présente invention fut décrite à titre purement indicatif et qu'elle peut recevoir plusieurs autres aménagements et variantes sans pour autant dépasser le cadre de la présente invention tel que délimité par les revendications qui suivent.

Les réalisations de l'invention au sujet desquelles un droit exclusif de propriété ou de privilège est revendiqué, sont définies comme suit:

1. Un jeu de hasard et d'argent sur ordinateur comprenant:

un billet de loterie de type instantanée sur lequel est inscrit une amorce et un code;

un programme d'ordinateur incluant des moyens de déchiffrage de l'amorce pour révéler un germe; un algorithme permettant de déterminer le déroulement et l'issue d'un jeu à partir dudit germe; et un jeu illustrant le déroulement et l'issue au joueur.

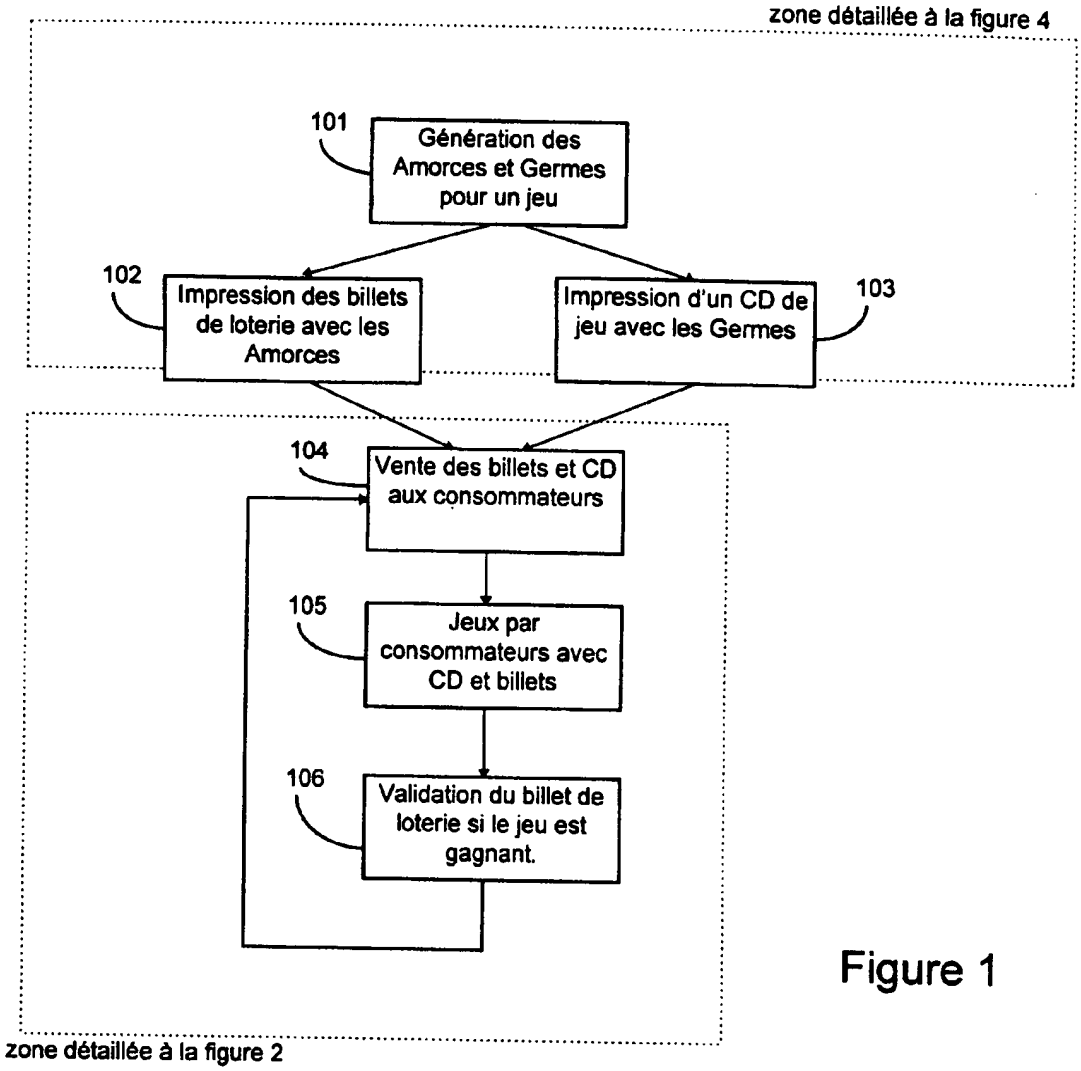

zone détaillée à la figure 4
101
Génération des Amorces et Germes pour un jeu
102
Impression des billets de loterie avec les Amorces
103
Impression d'un CD de jeu avec les Germes
104
Vente des billets et CD aux consommateurs
105
Jeux par consommateurs avec CD et billets
106
Validation du billet de loterie si le jeu est gagnant.
zone détaillée à la figure 2

Figure 1

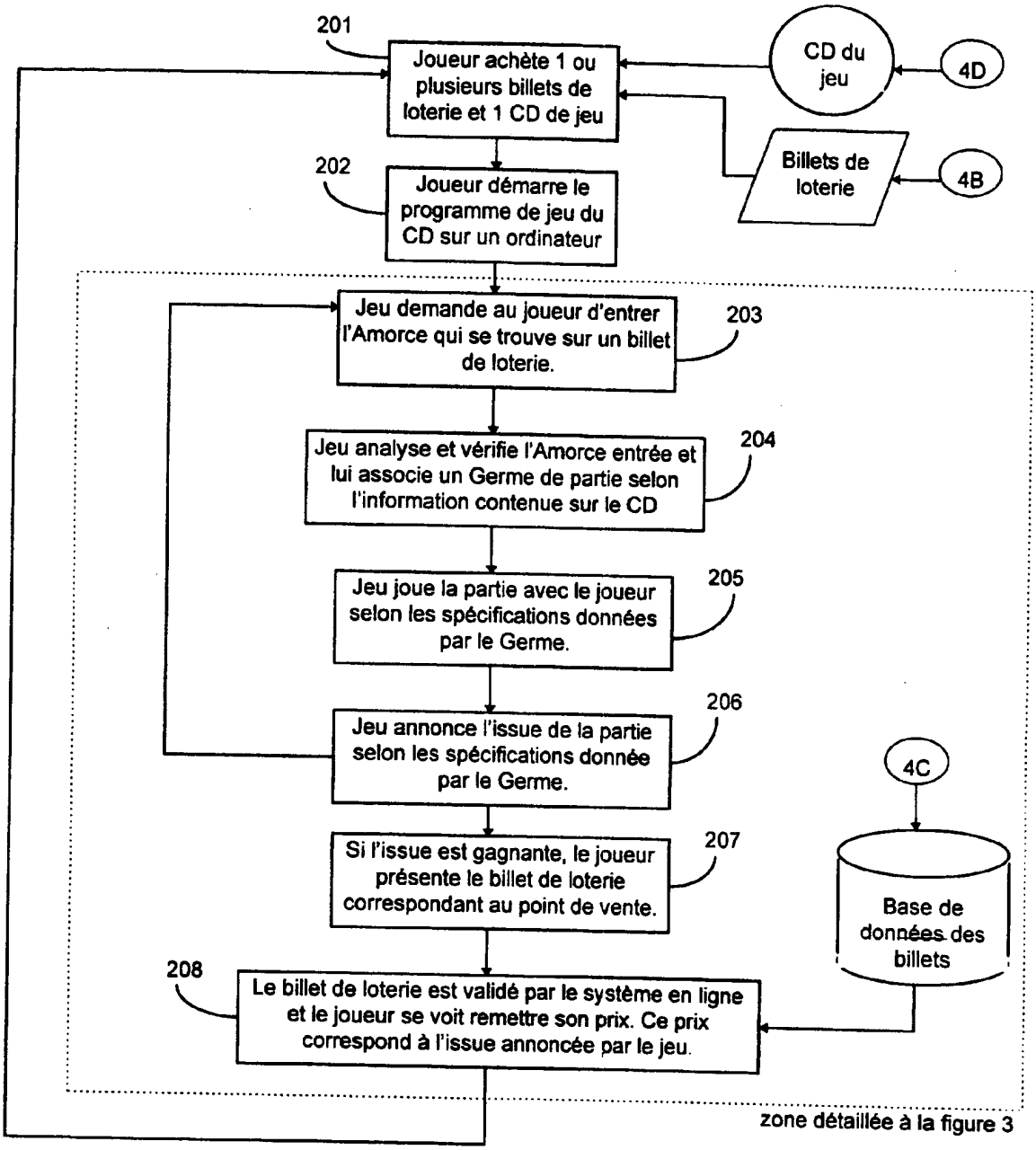

201
Joueur achète 1 ou plusieurs billets de loterie et 1 CD de jeu
CD du jeu
4D
Billets de loterie
4B
202
Joueur démarre le programme de jeu du CD sur un ordinateur
Jeu demande au joueur d'entrer l'Amorce qui se trouve sur un billet de loterie.
203
Jeu analyse et vérifie l'Amorce entrée et lui associe un Germe de partie selon l'information contenue sur le CD
204
Jeu joue la partie avec le joueur selon les spécifications données par le Germe.
205
Jeu annonce l'issue de la partie selon les spécifications donnée par le Germe.
206
4C
Si l'issue est gagnante, le joueur présente le billet de loterie correspondant au point de vente.
207
Base de données des billets
208
Le billet de loterie est validé par le système en ligne et le joueur se voit remettre son prix. Ce prix correspond à l'issue annoncée par le jeu.
zone détaillée à la figure 3

Figure 2

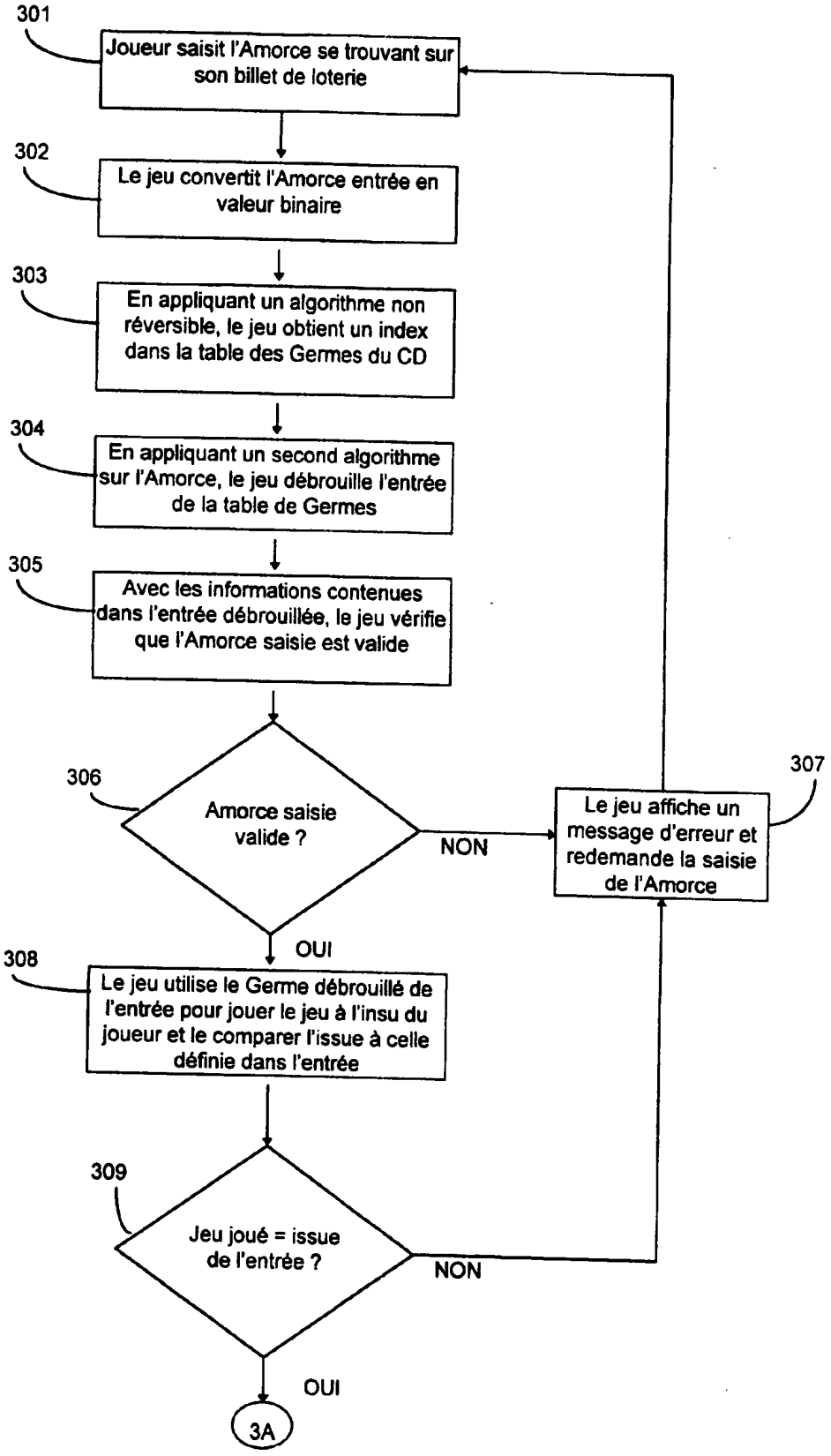

301
Joueur saisit l'Amorce se trouvant sur son billet de loterie
302
Le jeu convertit l'Amorce entrée en valeur binaire
303
En appliquant un algorithme non réversible, le jeu obtient un index dans la table des Germes du CD
304
En appliquant un second algorithme sur l'Amorce, le jeu débrouille l'entrée de la table de Germes
305
Avec les informations contenues dans l'entrée débrouillée, le jeu vérifie que l'Amorce saisie est valide
306
Amorce saisie valide ?
NON
307
Le jeu affiche un message d'erreur et redemande la saisie de l'Amorce
OUI
308
Le jeu utilise le Germe débrouillé de l'entrée pour jouer le jeu à l'insu du joueur et le comparer l'issue à celle définie dans l'entrée
309
Jeu joué = issue de l'entrée ?
NON
OUI
3A

Figure 3

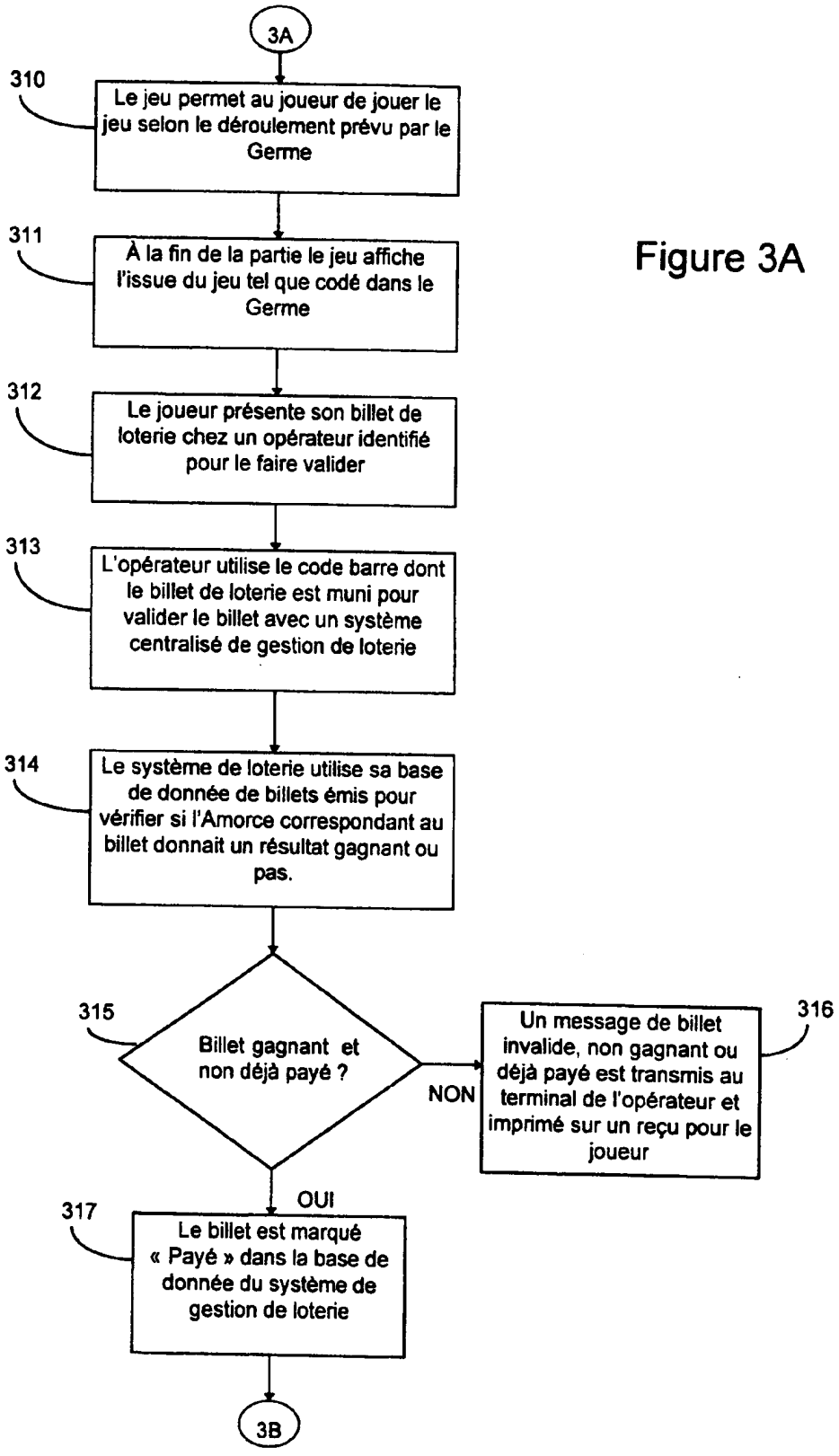

3A
310
Le jeu permet au joueur de jouer le jeu selon le déroulement prévu par le Germe
311
À la fin de la partie le jeu affiche l'issue du jeu tel que codé dans le Germe
312
Le joueur présente son billet de loterie chez un opérateur identifié pour le faire valider
313
L'opérateur utilise le code barre dont le billet de loterie est muni pour valider le billet avec un système centralisé de gestion de loterie
314
Le système de loterie utilise sa base de donnée de billets émis pour vérifier si l'Amorce correspondant au billet donnait un résultat gagnant ou pas.
315
Billet gagnant et non déjà payé ?
NON
316
Un message de billet invalide, non gagnant ou déjà payé est transmis au terminal de l'opérateur et imprimé sur un reçu pour le joueur
OUI
317
Le billet est marqué « Payé » dans la base de donnée du système de gestion de loterie
3B

Figure 3A

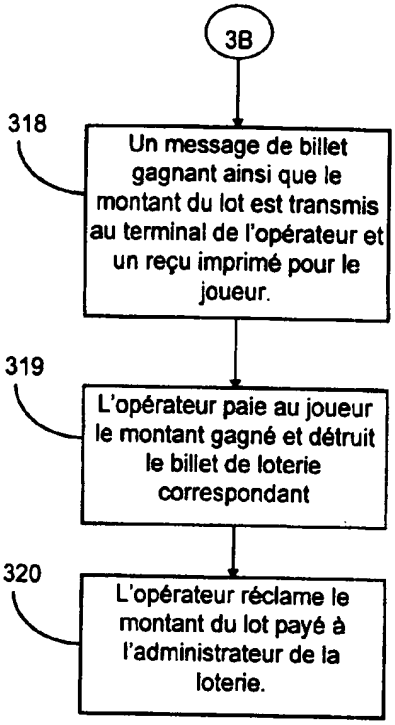

3B
318
Un message de billet gagnant ainsi que le montant du lot est transmis au terminal de l'opérateur et un reçu imprimé pour le joueur.
319
L'opérateur paie au joueur le montant gagné et détruit le billet de loterie correspondant
320
L'opérateur réclame le montant du lot payé à l'administrateur de la loterie.

Figure 3B

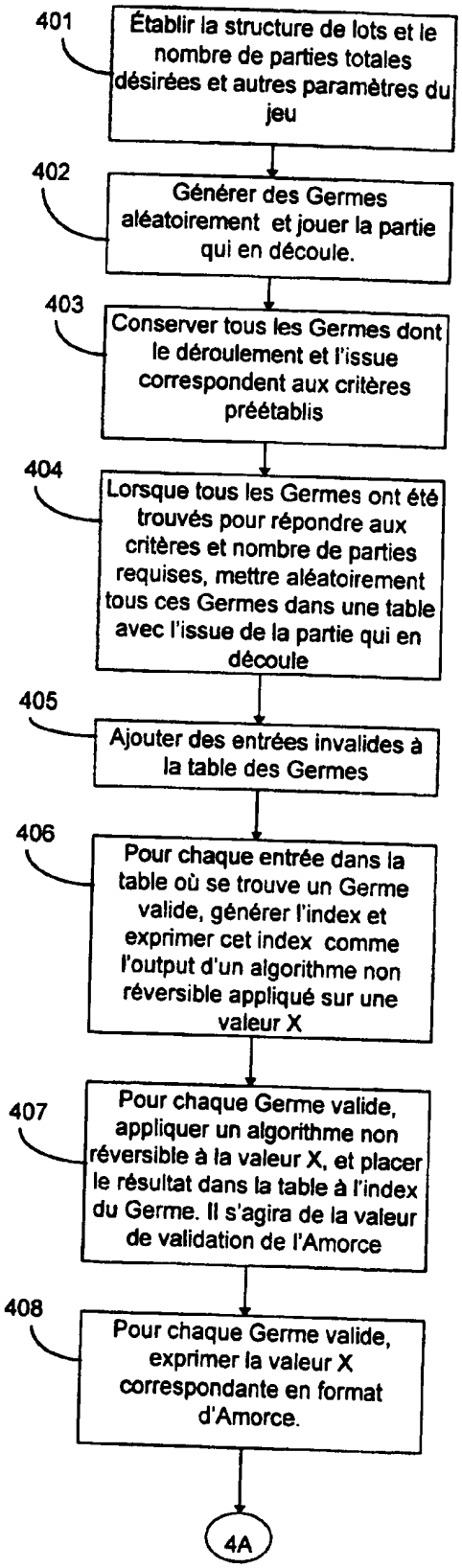

401
Établir la structure de lots et le nombre de parties totales désirées et autres paramètres du jeu
402
Générer des Germes aléatoirement et jouer la partie qui en découle.
403
Conserver tous les Germes dont le déroulement et l'issue correspondent aux critères préétablis
404
Lorsque tous les Germes ont été trouvés pour répondre aux critères et nombre de parties requises, mettre aléatoirement tous ces Germes dans une table avec l'issue de la partie qui en découle
405
Ajouter des entrées invalides à la table des Germes
406
Pour chaque entrée dans la table où se trouve un Germe valide, générer l'index et exprimer cet index comme l'output d'un algorithme non réversible appliqué sur une valeur X
407
Pour chaque Germe valide, appliquer un algorithme non réversible à la valeur X, et placer le résultat dans la table à l'index du Germe. Il s'agira de la valeur de validation de l'Amorce
408
Pour chaque Germe valide, exprimer la valeur X correspondante en format d'Amorce.
4A

Figure 4

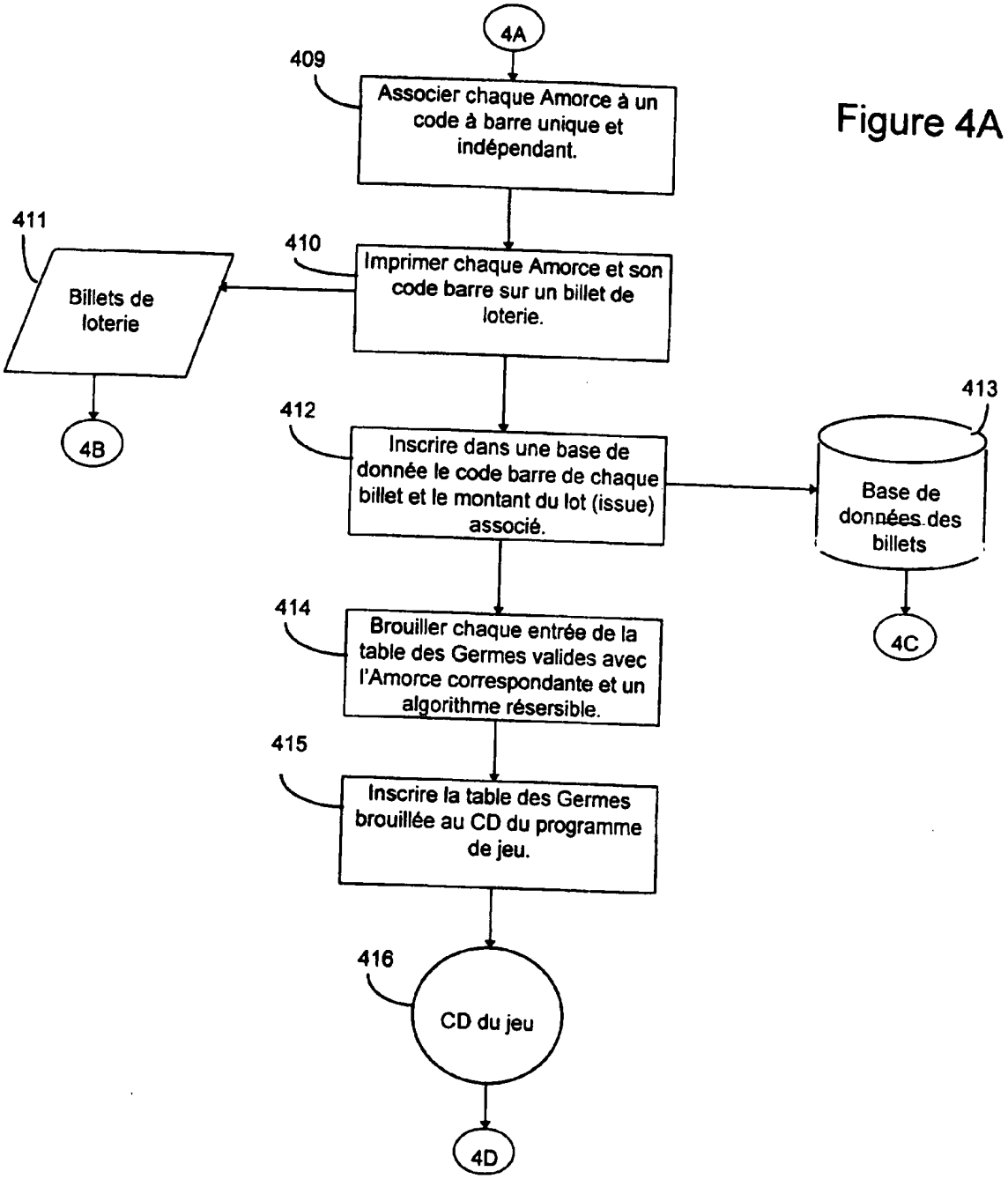
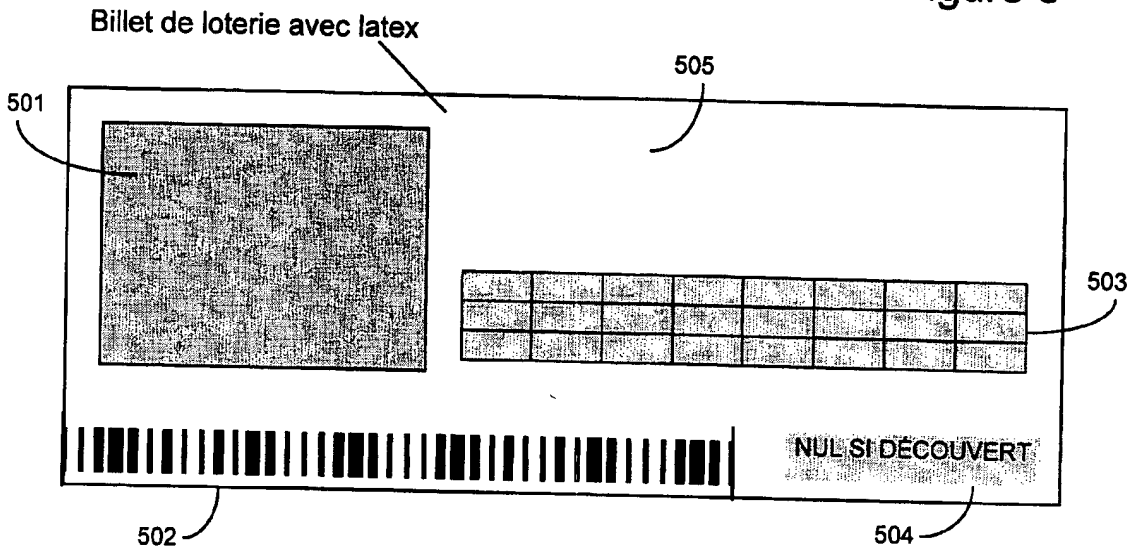

4A
409
Associer chaque Amorce à un code à barre unique et indépendant.
411
Billets de loterie
410
Imprimer chaque Amorce et son code barre sur un billet de loterie.
4B
412
Inscrire dans une base de donnée le code barre de chaque billet et le montant du lot (issue) associé.
413
Base de données des billets
4C
414
Brouiller chaque entrée de la table des Germes valides avec l'Amorce correspondante et un algorithme résersible.
415
Inscrire la table des Germes brouillée au CD du programme de jeu.
416
CD du jeu
4D

Figure 4A

Figure 5



Billet de loterie avec latex gratté

Figure 5A